Internet Wiretaps: Applying the Communications Assistance for Law Enforcement Act to Broadband Services

GENE D. PARK*

ABSTRACT

This article discusses the Federal Communications Commission's order to apply the standards of the Communications Assistance for Law Enforcement Act ("CALEA") to broadband Internet and voice over Internet Protocol providers, at the request of the Department of Justice and the Federal Bureau of Investigation. CALEA compliance would require such service providers to redesign their facilities to enable access points for law enforcement officials to easily wiretap communications under a court order. Industry and public policy groups have challenged the action. Although most organizations protesting the Order oppose it on grounds of cost and technological innovation, this article addresses some of the privacy implications of applying CALEA to the Internet. The discussion will proceed by detailing the origins of CALEA, and its specific provisions. Explanations and critiques are offered concerning the law enforcement rationale for making Internet providers CALEA-compliant. An overview is provided of the privacy implications, including the technical difficulties in isolating communications and the potential breach of such information by third parties. Finally, the statutory basis for the Federal Communications Commission's Order is reviewed, in light of the specific provisions of CALEA, its legislative history, and recent federal cases.

I. INTRODUCTION: THE FCC REQUIRES BROADBAND AND VOIP PROVIDERS TO COMPLY WITH THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

The Federal Communications Commission ("FCC") recently declared that broadband Internet providers and voice over Internet Protocol ("VoIP") services must have systems that allow law enforcement officials to feasibly implement wiretaps. In a Notice of Proposed Rulemaking (hereafter, the "Order")[1] issued on August 5,

---

* The author is a 2007 J.D. candidate at The Ohio State University Moritz College of Law. The author received a B.A. in English and political science from the University at Buffalo, the State University of New York in 2004.

[1] FEDERAL COMMUNICATIONS COMMISSION (FCC), IN THE MATTER OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT AND BROADBAND ACCESS AND SERVICES 1 (Aug. 5. 2005) *available at* http://www.askcalea.org/fcc/docs/20050923-fcc-05-153.pdf ("In this

2005, the FCC held that such entities were required to comply with the Communications Assistance for Law Enforcement Act ("CALEA").[2] Passed by Congress in 1994, CALEA mandated telecommunications carriers, predominantly telephone networks, to create design requirements to enable law enforcement to easily wiretap a criminal suspect in light of changing technology.[3] The Order represents the first step by the FCC to advance design mandates for providers of Internet broadband service and VoIP.[4]

Applying CALEA to the Internet has been the aim of law enforcement agencies, namely the Federal Bureau of Investigation ("FBI") and the Department of Justice ("DOJ"). Both agencies filed a joint petition to the FCC to apply CALEA to broadband Internet and VoIP providers.[5] In their petition, the agencies assert that a clear statutory construction of CALEA is necessary in order for the providers to conform to the requirements of the law.[6] The FBI and DOJ's primary interest is to promote national security in light of the difficulty of law enforcement to adapt to changing technology.[7] When

---

Order, we conclude that the Communications Assistance for Law Enforcement Act (CALEA) applies to facilities-based broadband Internet access providers and providers of interconnected voice over Internet Protocol (VoIP) service.") [*hereinafter* FCC].

[2] Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001-1010 (1994).

[3] FCC, *supra* note 1, at 2 ("CALEA was intended to preserve the ability of law enforcement agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities.").

[4] *Id.* at 13 (The FCC defines "broadband" as "those services having the capability to support upstream or downstream speeds in excess of 200 kilobits per second (kbps) in the last mile." VoIP services, according to the FCC, includes real-time, offer two-way communications that require the user to have a broadband connection in order to make calls on the public telephone network).

[5] U.S. DEP'T OF JUSTICE (DOJ), JOINT PETITION FOR EXPEDITED RULEMAKING III (March 10, 2004), *available at* http://www.askcalea.net/pet/docs/20040310.calea.jper.pdf.

[6] *Id.* at 9 ("[T]he Commission can resolve any controversy about CALEA's applicability to broadband access, broadband telephony, and push-to-talk dispatch services separately and independently from its proceedings . . .").

[7] *Id.* at 8-9 ("The importance and the urgency of this task cannot be overstated. The ability of federal, state, and local law enforcement to carry out critical electronic surveillance is *being compromised today* by providers who have failed to implement CALEA-compliant intercept capabilities. Communications among surveillance targets are being lost and associated call-identifying information is not being provided in the timely manner required by CALEA.").

formulating the Order, the FCC largely accepted the rationale and the proposals of the agencies.

The expansion of CALEA to broadband providers, however, has encountered strong criticism from a variety of industrial, educational, and public interest organizations. In response to the Order, these groups, consisting of the American Council on Education ("ACE"), Center for Democracy and Technology ("CDT"), the Electronic Frontier Foundation ("EFF"), the Electronic Privacy Information Center ("EPIC"), the American Library Association, and Sun Microsystems, among others, filed a petition in the United States Court of Appeals for the District of Columbia Circuit for a review of the Order.[8] On June 9, 2006, the Court ruled in favor of the FCC in *American Council on Education v. FCC*, holding that the agency's interpretation of CALEA and its view that broadband and VoIP providers were telecommunications carriers covered under the law, was a "reasonable policy choice."[9]

The immediate publicity surrounding the release of the Order concerned the substantial cost this would place on broadband providers, particularly on educational institutions. Broadband providers were expected to bear the brunt of implementing the design modifications in order to make their facilities CALEA compliant – as a consequence, the FCC's Order has been dubbed "the mother of unfunded mandates."[10] The cost for universities to implement the plan is estimated at $7 billion, and ACE believes that students will bear the burden through tuition increases.[11] Upon review of the decision of the D.C. Circuit, ACE believes that most higher education institutions are largely exempt from the Order because their Internet connections qualify as "private networks;" as private networks, they are excluded

---

[8] Petition for Review, Comptel v. Fed. Communications Comm'n, 1 (October 25, 2005), *available at* http://www.cdt.org/digi_tele/20051025caleapetition.pdf ("Petitioners seek relief from the Order on the grounds that is exceeds the Commission's statutory authority and is arbitrary, capricious, unsupported by substantial evidence, and contrary to law.").

[9] American Council on Education v. FCC, 451 F.3d 226, 232 (D.C. Cir. 2006).

[10] Sam Dillon & Stephen Labaton, *Colleges Oppose Call to Upgrade Online Systems*, N.Y. TIMES, Oct. 23, 2005, at A1, *available at* http://www.nytimes.com/2005/10/23/technology/23college.html?ex=1131339600&en=42afaa66fad5aa70&ei=5070&hp.

[11] *Id.* (according to Terry W. Hartle, senior vice president at the American Council on Education, the result of cost of the design modifications would result in at least a $450 tuition increase per student).

from CALEA's coverage and would not have to bear substantial costs.[12]

The FCC's August 5 Order represents the first notice announcing the requirements of the regulation. Affected entities will have eighteen months following the issuance of the Order to comply.[13] After a comment period, the FCC will issue another order to address specific questions regarding implementation.[14] An exemption for educational institutions is possible,[15] but the FCC's description of the subsequent order makes it clear that there is no open question regarding the inevitability of the regulation. Considerations on the rule will only concern its implementation to broadband and VoIP providers, not its applicability.[16]

The relevance of the FCC's Order has increased following the disclosure of the National Security Agency's domestic wiretapping policy, authorized by President George W. Bush.[17] Telecommunications corporations that are required to comply with law enforcement wiretap requests reportedly rely on an attorney general certification, instead of a court order.[18] Arguably, CALEA "has created a thriving 'lawful intercept' industry for technology to make

---

[12] *The Application of CALEA to Higher Education Networks*, AMERICAN COUNCIL ON EDUCATION (July 13, 2006), *available at* http://www.acenet.edu/AM/Template.cfm?Section=Search&section=Legal_Issues_and_Policy_Briefs1&template=/CM/ContentDisplay.cfm&ContentFileID=1827 [hereinafter *Application*].

[13] FCC, *supra* note 1, at 2 ("Because we acknowledge that providers need a reasonable amount of time to come into compliance with all relevant CALEA requirements, we establish a deadline of 18 months from the effective date of this Order, by which time newly covered entities and providers of newly covered services must be in full compliance."). The effective date and the end of the comment period was November 14, 2005.

[14] *Id.* ("This subsequent order will include other important issues under CALEA, such as compliance extensions and exemptions, cost recovery, identification of future services and entities subject to CALEA, and enforcement.").

[15] Dillon & Labaton, *supra* note 10, at A1.

[16] FCC, *supra* note 1, at 2.

[17] Scott Shane, *Attention in N.S.A. Debate Turns to Telecom Industry*, N.Y. TIMES, Feb. 11, 2006, at A1, *available at* http://www.nytimes.com/2006/02/11/politics/11nexus.html.

[18] *Id.*

eavesdropping easier."[19] The closeness of the relationship between the telecommunications industry and the intelligence agencies has come under scrutiny.[20]

Besides the cost, critics of extending CALEA to broadband providers oppose the regulation for the following reasons. Critics argue the FCC is exceeding the statutory scope of the law to apply CALEA to broadband providers.[21] Also, they charge that because modifying current equipment for CALEA compliance imposes huge costs and burdens that are difficult for the providers to bear, the regulation inhibits technological innovation, and forces businesses to look overseas.[22]

In regards to privacy concerns, critics argue that expanding CALEA to the Internet would expose the communications of many law-abiding individuals to both law enforcement agents and third parties.[23] The method in which information is distributed over the Internet, through data packets, presents difficulties in isolating specific communications directed for extraction under a court order. The creation of access points within the architecture of the Internet may also allow unauthorized access into private communications.

---

[19] *Id.*

[20] *Id.* ("Some companies are said by current and former government officials to have provided the eavesdropping agency access to streams of telephone and Internet traffic entering and leaving the United States . . . . Now the companies are in an awkward position, with members of Congress questioning them about their role in the eavesdropping. On Thursday two Democratic senators, Edward M. Kennedy of Massachusetts and Russell D. Feingold of Wisconsin, wrote to the chief executives of AT&T, Sprint Nextel and Verizon, asking them to confirm or deny a report in USA Today on Monday that said telecommunications executives had identified AT&T, Sprint and MCI (now part of Verizon) as partners of the agency.").

[21] *See* Petition for Review, *supra* note 8, at 2.

[22] *See* Associated Press, *Groups Slam FCC on Internet Phone Tap Rule: Regulations May Make Systems More Vulnerable to Hackers*, MSNBC, Aug. 10, 2005, http://www.msnbc.msn.com/id/8900665/ ("'Creativity and innovation will end up moving offshore where programmers outside the U.S. can develop technologies that are not required to address the onerous CALEA requirements,' said Kurt Opsahl, staff attorney at the Electronic Frontier Foundation. 'The U.S. companies will face competition from foreign providers who will enjoy an advantage.'") [hereinafter *Groups*].

[23] *See* Electronic Frontier Foundation (EFF), CALEA: Frequently Asked Questions, http://www.eff.org/Privacy/Surveillance/CALEA/?f=faq.html (last visited March 3, 2006) ("Congress has noted that 'wiretaps . . . are potentially more penetrating, less discriminating, and less visible than ordinary searches.' This makes wiretaps an extremely powerful investigative tool for law enforcement, but also highly invasive of individuals' privacy.").

II. BACKGROUND OF THE CREATION OF CALEA

In order to understand the implications, the alleged necessity, and the criticism of the Order, it is necessary to analyze the background on the creation of CALEA and the law of wiretaps. A little over a decade old, CALEA itself has roots that extend back to the first major ruling on the constitutional use of wiretaps. In the *Katz* decision, the Supreme Court held that the law enforcement investigative activity of tapping a phone and listening to the conversation was a search under the Fourth Amendment.[24] Consequently, all requests for wiretaps need probable cause and warrants prior to their use.

In light of this holding, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, which contained important provisions regarding the use of wiretaps in Title III.[25] A general prohibition was made against unauthorized electronic eavesdropping by individuals or law enforcement agents without a warrant in compliance with Title III procedures.[26] Wiretaps were deemed permissible for certain predicate offenses under the statute.[27] To this very day, law enforcement agents have been able to use wiretaps under different technological mediums, including the Internet, under Title III procedures.[28]

CALEA was never meant to expand the scope of law enforcement power under the Title III requirements. It was developed at the behest of law enforcement agencies to more easily implement the provisions of Title III.[29] Changes in phone technology largely brought about the

---

[24] U.S. v. Katz, 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

[25] 18 U.S.C. § 2510-2520 (Supp. V. 1968).

[26] *Id.* § 2511.

[27] *Id.* § 2516.

[28] EFF, *supra* note 23 ("Even before CALEA, federal law required communication service providers to assist law enforcement in carrying out the interception of communications (whether via telephone or computer network). . . [i]f law enforcement can meet the strict standards of Title III.").

[29] U.S. DEP'T OF JUSTICE, US ATTORNEY'S BULLETIN: COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT (CALEA) (Apr. 26, 2005), *available at* http://www.usdoj.gov/criminal/cybercrime/usamay2001_4.htm ("Although Title III required

necessity for CALEA, a law mandating design requirements on to the phone companies; at the time of its passage, telephone networks were switching to digital systems, which created problems for law enforcement officials in implementing wiretaps.[30] New technology was necessary.

> Digital phone systems no longer had a wire to tap, at least not at the phone company office. Instead, some kind of digital device, like a computer, had to be used to intercept conversations and CALEA required telecommunications companies to provide such an interface for law enforcement use.[31]

The state of technology at the time made it evident to Congress what was needed for successful implementation of Title III wiretaps: telecommunications providers had to accommodate law enforcement officials to quickly apply their systems to new technology.[32]

III. THE PROVISIONS OF CALEA

As a result of this history, CALEA is a statute mandating entities to modify their structures to allow law enforcement officials to readily install wiretaps on individuals under criminal investigation.[33]

One important consideration is to determine who is covered by CALEA. The capability requirements of CALEA state that "a telecommunications carrier shall ensure that its equipment, facilities,

---

telecommunications carriers to provide 'any assistance necessary to accomplish an electronic interception,' 18.U.S.C. § 2518[4], the question of whether telecommunications carriers had an obligation to design their networks such that they did not impede a lawfully- authorized interception had not been decided.").

[30] Ctr. for Democracy and Technology, Coalition Opposes Net Wiretap Design Mandates (Nov. 10, 2004), http://www.cdt.org/publications/pp_10.20.shtml (CALEA was "enacted to address concrete and documented problems carrying out wiretaps of phone conversations as digital switches and other new features were being introduced within the traditional telephone network, or PSTN.").

[31] Philip Baczewski, *Federal Eavesdropping: Coming to an Internet Near You*, BENCHMARKS ONLINE, Nov. 2005, http://www.unt.edu/benchmarks/archives/2005/november05/netcom.htm.

[32] Details of the legislative history of CALEA is located in Part E, Section 2 of this article.

[33] 47 U.S.C. § 1001(2).

or services that provide a customer or subscriber with the ability to" immediately isolate and capture requested communications and call-identifying information.[34] A telecommunications carrier under CALEA is defined under the following provision.

> (8) The term "telecommunications carrier:"
>
> (A) means a person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire; and
>
> (B) includes--
>
> (ii) a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this [chapter].[35]

The traditional telephone providers – the Public Switching Technology Networks ("PSTN") – were considered telecommunications carriers under CALEA and subject to its design requirements.[36] The "substantial replacement" provision of a telecommunications carrier under 47 U.S.C. § 1001(8)(b)(ii) has particularly important implications for the construction of the current Order – an issue later explored in this article.

Similarly, it is important to note which entities are not covered under CALEA. The definition of a telecommunications carrier in 47 U.S.C. § 1001(8)(c)(i) excludes "persons or entities insofar as they are engaged in providing information services." "Information services" under CALEA is defined here:

---

[34] Communications Assistance for Law Enforcement Act ("CALEA"), 47 U.S.C. § 1002(a) (1994).

[35] 47 U.S.C. § 1001(8).

[36] *See* FCC, *supra* note 1, at 8 (The FCC disputes the notion that CALEA was strictly meant to apply to apply to the PSTN at the time of CALEA's enactment in 1994).

> (A) [Information service] means the offering of a capability for
>
> generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and
>
> (B) includes—
>
> (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;
>
> (ii) electronic publishing; and
>
> (iii) electronic messaging services.[37]

The capability requirements under CALEA in 47 U.S.C. § 1002(b)(2)(a) state that information services are exempt from designing and maintaining access points for law enforcement officials.[38] As detailed later in this article, the applicability of the Internet as an "information service," and broadband Internet providers in particular, is a crucial question in regards to the recent Order.

The capability requirements of CALEA in 47 U.S.C. § 1002(a) mandate telecommunication carriers to maintain facilities that can "expeditiously" isolate all wire and electronic communications, and call-identifying information that the carrier already provides to the subscriber of the service.[39] Among the other provisions of CALEA, 47 U.S.C. § 1004 requires that telecommunications carriers maintain systems that keep secure the contents of the communication and the call-identifying information, so that only a law enforcement officer

---

[37] 47 U.S.C. § 1001(6).

[38] *Id.* § 1002(b)(2)(a).

[39] *Id.* § 1001(2) ("'[C]all-identifying information' means dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier.").

acting in accordance with a court order, or a carrier employee can intercept such information.[40]

Regarding the specific technical requirements necessary under CALEA, the statute states that the Attorney General, through law enforcement agencies, shall consult with representatives of the telecommunications industries to determine what specific designs are necessary.[41] In practice, this has meant that the Telecommunications Industry Association ("TIA") has developed the standards to determine how carriers can assist law enforcement agencies to implement the wiretap requirements of CALEA.[42] The statute also contains specific enforcement provisions for the act under 47 U.S.C. § 1007, which includes evaluating the totality of the circumstances of whether a telecommunications carrier is in fact capable of complying with the Act, and the countervailing policy reasons that factor into the consideration.[43]

IV. THE LAW ENFORCEMENT RATIONALE FOR APPLYING CALEA TO BROADBAND AND VOIP PROVIDERS.

Konrad Trope, an attorney who practices in cyberspace and intellectual property law and is a member of the California State Bar Committee on Cyberspace, sums up the law enforcement rationale for extending CALEA to the Internet:

> federal law enforcement agencies worry that unless Internet service providers, and in particular VoIP providers, offer surveillance hubs based on common standards, lawbreakers

---

[40] *Id.* § 1004.

[41] *Id.* § 1006. (The "consultation" provision of CALEA is one component of its safe harbor section).

[42] EFF, *supra* note 23.

[43] 47 U.S.C. § 1008 (The relevant provision, 47 U.S.C. § 1008(b)(1), weighs: "(A) The effect on public safety and national security, (B) The effect on rates for basic residential telephone service, (C) The need to protect the privacy and security of communications not authorized to be intercepted, (D) The need to achieve the capability assistance requirements of section 1002 of this title by cost-effective methods. (E) The effect on the nature and cost of the equipment, facility, or service at issue, (F) The effect on the operation of the equipment, facility, or service at issue. (G) The policy of the United States to encourage the provision of new technologies and services to the public," among others).

> can evade or, at the very least, complicate surveillance by using VoIP providers such as Vonage, Time Warner Cable, Net2Phone, 8X8, deltathree and Digital Voice.[44]

In their joint petition, the FBI and the DOJ view the extension of CALEA to broadband and VoIP providers as a matter of necessity.[45] It is necessary in order to combat technologically proficient criminals who may use the Internet to more easily flout the wiretap laws.[46] As explained in the joint petition, "electronic surveillance is an invaluable and necessary tool for federal, state, and local law enforcement in their fight to protect the American public against criminals, terrorists, and spies."[47] Under their understanding of legislative intent, it was the purpose of Congress, by enacting CALEA, to allow law enforcement to continue to conduct electronic surveillance by continually defining the telecommunications carriers' duties to comply with the design requirements of the act.[48]

The Order accepts the necessity reasoning that lies behind the joint petition. In the Order, the FCC states, "[i]n addition, covering all broadband Internet access service providers prevents migration of criminal activity onto less regulated platforms."[49] The FCC reasons it ultimately serves the public interest to prevent criminals and terrorists from avoiding law enforcement surveillance by using broadband Internet as a substitute for dial-up service.[50] In a separate opinion which accompanied the Order, Commissioner Kathleen Q. Abernathy states, "[l]ast year the Department of Justice . . . brought to our

---

[44] Konrad Trope, *The Technology Trade,* FINDLAW (Feb. 2004), http://practice.findlaw.com/tooltalk-0204.html.

[45] DOJ, *supra* note 5, at 71.

[46] *Id.*

[47] *Id.*

[48] *Id.* ("Congress enacted CALEA to preserve law enforcement's ability to conduct lawful electronic surveillance despite changing telecommunications technologies by further defining the telecommunications industry's existing obligation to provision lawful electronic surveillance capabilities and requiring industry to develop and deploy CALEA intercept solutions.").

[49] FCC, *supra* note 1, at 17.

[50] *Id.* at 18.

attention ways in which the Commission might act to further this goal by closing gaps in the application of CALEA – gaps that increase the danger posed to American citizens by criminals and terrorists."[51] Citing Title I of the Communications Act, applying CALEA to broadband providers would promote the "safety of life and property through the use of wire and radio communications."[52]

The effect of the Order would presumably stymie the specific problem of law enforcement agencies – the loss of key communications and call-identifying information due to providers that lack facilities readily capable of providing immediate backdoor access for wiretaps. According to these agencies, "[t]hese problems are real, not hypothetical, and their impact on the ability of federal, state, and local law enforcement to protect the public is growing with each passing day."[53]

Critics of the Order, however, are more skeptical of the actual necessity to extend CALEA to broadband providers for the purposes of national security. They note the absence of specific examples in the joint petition that state instances of lost data due to the lack of CALEA compliance on the part of broadband providers, the current ability for such entities to assist law enforcement wiretap requests, and the lack of a demonstrable need to utilize Internet wiretaps.

Public interest groups contend that Internet wiretaps have been implemented effectively under the framework of Title III and there is no basis for asserting that there has been a lack of compliance with the wiretap orders. The Center for Democracy and Technology ("CDT") argues in their own response to the joint petition that there was no proof that law enforcement was having any investigatory difficulties due to the lack of CALEA compliance.[54] CDT argues that service providers have by-and-large readily met the demands of law enforcement wiretap requests.[55] As examples of technological compliance, CDT cites:

---

[51] *Id.* at 54.

[52] *Id.*

[53] DOJ, *supra* note 5, at 9.

[54] JOINT COMMENTS OF INDUSTRY AND PUBLIC INTEREST, IN THE MATTER OF COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT AND BROADBAND ACCESS AND SERVICES 4 (Nov. 8, 2004), *available at* http://www.cdt.org/digi_tele/20041108indpubint.pdf [*hereinafter* Joint Comments].

[55] *Id.* at 4-5.

- The Telecommunications Industry Association ("TIA") has completed Revision B of its J-Standard 025 for packet communications, and is working on Revision C.

- Cisco, a major maker of Internet routing equipment, already offers an interception capability in its equipment.

Indeed, according to the FBI's own 'AskCALEA' web site, there are at least *seven* different completed or on-going technical standards efforts aimed at facilitating interception of Internet communications.[56] CDT then concludes, in light of the industry's apparent de facto compliance with CALEA, and in light of the lack of actual examples of surveillance difficulties with broadband providers, that "[s]imply stated, law enforcement agencies have presented *no* evidence of any difficulty that they have actually encountered that would be solved by the extension of CALEA to the Internet or Internet applications."[57] An FCC ruling favorable to the joint petition's arguments, CDT contends, would have no foundation in "reasoned decisionmaking" that is the basis of the agency's authority.[58] The apparent vagueness of the joint petition's claim – that crime-fighting techniques are compromised due to the lack of CALEA compliance – is similarly assailed.[59]

Education advocates, mirroring these reasons, argue that the current infrastructure of their broadband facilities is already amenable to law enforcement requests, and moreover, there is no major need to

---

[56] *Id.* at 5.

[57] *Id.* at 6.

[58] *Id.*

[59] *See Summary of DOJ Petition for Rulemaking to Expand the CALEA to Cover Information Services*, TECH L. J. (April 9, 2004), http://www.techlawjournal.com/topstories/2004/20040409.asp ("The DOJ petition also complains that some entities claim that they are not subject to the requirements of the CALEA. However, the petition is silent as to who these entities are. Nor does the petition enumerate the types of entities that cause it concern. The DOJ wrote the key sentence quoted above in the passive mood -- "surveillance is being compromised" -- thereby evading the revelation of who is compromising surveillance." [hereinafter *Summary*].

accommodate them in the first place.[60] Educause, a technology-in-education advocacy group, explains the current system that exists to grant Title III wiretap requests in the following fashion.

> This normally involves law enforcement personnel coming to campus, bringing the necessary equipment with them, and working with the campus IT department to isolate the necessary communications. Law enforcement has expressed several problems with this, mainly that it is expensive and very time consuming...has been known to take weeks to find and isolate the correct information.[61]

More to the point, the group noted that in an informal survey, no orders were issued to universities in 2003.[62]

VoIP providers make similar arguments. Jeff Pulver, the creator of Free World Dial-up, a VoIP provider and one of the petitioners that filed against the Order, believes the current system of voluntary compliance shows de facto fulfillment of CALEA's goals: "[w]e have our chance right now to prove to law enforcement that we can do this on a voluntary basis."[63]

The criticism of the law enforcement necessity argument is also based on the comparatively few wiretap orders actually issued for the Internet. CDT cites that only twelve out of the 1,442 wiretaps issued for 2003 involved computer communications.[64] Wiretap orders for 2004 do not report any significant demand for tapping computers. Of the 1,710 wiretap orders, only twelve were issued for computers.[65]

---

[60] Educause, *CALEA General Frequently Asked Questions*, http://www.educause.edu/content.asp?page_id=9355&bhcp=1 (last visited March 3, 2006).

[61] *Id.*

[62] *Id.*

[63] Declan McCullagh & Ben Charney, *FBI Adds to Wiretap Wishlist* (March 12, 2004), CNET NEWS.COM, http://news.com.com/2100-1028_3-5172948.html.

[64] Joint Comments, *supra* note 54, at 6 (citing the Report for the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications, issued April 30, 2004, *available at* http://www.uscourts.gov/wiretap03/contents.html.).

[65] Report for the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or

CDT also denies the notion that modifying CALEA in the proposed manner will have any actual deterring effect on "tech-savvy criminals." In disputing this assumption, CDT suggests that any criminal savvy enough to know what the Order covers, and more notably, what technologies it does not cover, will simply rely on the latter to undertake his criminal activities.[66]

E. THE PRIVACY IMPLICATIONS OF APPLYING CALEA TO THE INTERNET

Although the Order would not and could not expand any of the existing wiretap laws to the Internet, critics of the plan argue that privacy interests are threatened by creating access points for law enforcement. Privacy advocates have based their arguments on the fact that the Internet serves a different purpose and is technologically dissimilar to landline phone services, the original medium of communication CALEA intended to cover.

The Internet deserves different treatment from the phone networks, it is argued, primarily because of the type of private information available. In her article covering online surveillance, Susan Freiwald, a professor at the University of San Francisco School of Law, writes:

> [W]e reveal more of ourselves online than on the telephone, because we are more clearly identified with our Internet activities via our password-protected accounts. We transmit much richer information online than offline; in addition to conversations, we send pictures, videos, songs, and long documents. We also create records of our activities when we shop, read, play, organize, and date online.[67]

A large amount of private activity thus occurs on the Internet. The Internet is open and decentralized, as opposed to phone networks

---

Electronic Communications 9-10, *available at* http://www.uscourts.gov/wiretap04/2004WireTap.pdf.

[66] Joint Comments, *supra* note 54, at 10.

[67] Susan Friewald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 77 (2004).

which are managed centrally. These constitute reasons for a cautious approach to applying wiretaps to the Internet.[68]

Problems are presented with the exposure of this information under CALEA, due to the Internet's use of data packets as its mode of communication.[69] CALEA's capability requirements make a distinction between communications and call-identifying information.[70] The distinction rests on the Title III treatment of the content of intercepted communications (phone conversations), which typically is afforded the highest protections under the law, and traditional call-identifying information, such as dialing and routing data.[71] Such distinctions, however, are legally and technologically definable with ease: the phone networks by nature are closed and centralized, where all conversations between two parties traveled along a set path.[72]

Information on the Internet is distributed in data packets, which travel not on a set path, but by whatever route is available.[73] Content is therefore broken up and distributed en route to the recipient's computer.[74] The EFF points out that the fine distinction between

---

[68] Jack X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 83 (1997) ("As an intentionally open system of linked computers, the Internet is inherently insecure. The dramatic development of the Internet as a networked global communications medium and the expansion in the range of transactions that occur on-line have produced a qualitative change in the nature of communications and, accordingly, in the nature and amount of the information that is exposed to both lawful interception and illegal intrusion or misuse.").

[69] EFF, *supra* note 23.

[70] 47 U.S.C. § 1002(a)(1) requires the isolation of "communications," while 47 U.S.C. § 1002(a)(2) requires the isolation of call-identifying information.

[71] Dempsey, *supra* note 68, at 83.

[72] Sunny Lu, Note, *Cellco Partnership v. FCC & Vonage Holdings Corp. v. Minnesota Public Utilities Commission: VoIP's Shifting Legal and Political Landscape*, 20 BERKELEY TECH. L.J. 859, 873 (2005).

[73] *What is A Packet,* HOWSTUFFWORKS, http://computer.howstuffworks.com/question525.htm (last visited Jan. 10, 2006).

[74] For a detailed explanation of the technical process involved in the transmission of Internet communications and its implications under CALEA, *see* Susan Landau, *Security, Wiretapping, and the Internet*, IEEE SECURITY AND PRIVACY 30 (November/December 2005), *available at* http://research.sun.com/people/slandau/SWatI.pdf ("On the Internet, routing control is distributed. It's impossible to determine a priori the routing of the packets the

content and call-identifying information ("signaling information" when the term is applied to the Internet) in CALEA is muddled when applied to the Internet.[75] The structure of the transmission, via the seven protocol layers, makes it unclear where information is contained within the transmission.[76] The concern is that the lower standard used to find signaling information could result in the exposure of content information, and thus invade the privacy of individuals.[77] The EFF states, "[a]s the FCC concedes, broadband access providers may not be able to easily isolate call-identifying information without examining the packets in detail, which would necessarily require examining the packet content."[78]

Susan Landau, a Sun Microsystems Laboratories engineer, and a member of the National Institute of Standards and Technology's Information Security and Privacy Advisory Board, explains the difficulty the architecture of the Internet presents in securing private communications: "unless the communication is tapped at the endpoints (at the user, or at the Internet service provider if the user always accesses the same provider), it's impossible to guarantee 100 percent access to all communication packets."[79] Monitoring communications via a gateway for law enforcement through the routers of an Internet service provider can expose communications other than those specified within a court order.[80]

CALEA also explicitly states that call-identifying information "shall not include any information that may disclose the physical location of the subscriber."[81] The CDT argues that the potential for

---

communication is broken into—this is determined by the routing tables, which change depending on the network traffic.").

[75] EFF, *supra* note 23.

[76] *Id.* ("[I]n the packet-mode world of the Internet, communications are encapsulated ... and each protocol layer is associated with different 'signaling information.' Whether a component is 'signaling information' or 'content' depends on which layer is reading it.").

[77] *Id.*

[78] *Id.*

[79] Landau, *supra* note 74, at 30.

[80] *Id.*

[81] 47 U.S.C. § 1002(a)(2)(B).

the exposure of a person's physical location exists through the use of an Internet wiretap, and thus conflicts with CALEA's own provision.[82] An individual's Internet Protocol ("IP") address (or in the case of VoIP, the Session Initiation Protocol data) may reveal a person's identity, since IP addresses are occasionally registered through an individual's name.[83] This information may exist on the WHOIS database, which reveals the person's physical location.[84]

The problem, as previously explained, stems from the disperse method data packets that are distributed through the Internet, as well as the multiple protocol layers that embed both signaling information and content.[85] Web site addresses, times, and server information surround the content of the information, making a distinction between isolating signaling information and content both technically and legally difficult.[86] Trust is then placed in the hands of law enforcement to extract the information as particularized in the court order.[87]

One significant lower court authority has provided the FCC with both limits and discretion in the implementation of CALEA relating to signaling information. In *United States Telecom Association v. FCC*, the Court of Appeals for the District of Columbia Circuit found that the FCC had not fulfilled its burden of using "reasoned decision-making" to justify proposals made on an FBI "punch list."[88] The "punch list" consisted of recommendations the FBI argued were lawful under CALEA, including "telephone numbers of calls

---

[82] Joint Comments, *supra* note 54, at 46.

[83] *Id.* at 47.

[84] *Id.*

[85] David Crowe, *CALEA: US Communications Assistance for Law Enforcement Act*, WIRELESS SECURITY PERSPECTIVES (Nov. 15, 2001), *available at* http://www.cnp-wireless.com/ArticleArchive/Wireless%20Review/20011115WR-CALEA.html.

[86] *Id.*

[87] *Id.* ("The simplest approach for the industry is to send the entire packet to law enforcement, trusting them to determine the protocol, extract the identifying information and throw the content away for court orders not allowing its collection. This is currently being treated as a technical problem, but in reality it is a failure of legislators to provide laws attuned to packet-based methods of communications.").

[88] United States Telcom Ass'n v. FCC, 227 F.3d 450, 460 (D.C. Cir. 2000).

completed using calling cards as well as signaling information related to custom calling features such as call waiting and conference calling."[89] The Court held that without explaining the rationale for implementing these requirements, especially without consultation with the telecommunications industry as required by CALEA, the FCC's order could not stand.[90]

The court, however, also refused to question the FCC's decision to subject "packet-switching technology" to CALEA.[91] The decision was not based on Internet technology but wireless telephone calls.[92] The Court found that the FCC complied with CALEA because its decision was based on the recommendation of the TIA, the organization law enforcement, and the FCC consult to implement CALEA technology standards under 47 U.S.C. § 1006(b).[93] The Court rejected the claims of the privacy rights litigants who argued that the FCC violated the requirement of 47 U.S.C. § 1002(a)(4), which mandates the FCC to "protect the privacy and security of communications not authorized to be intercepted."[94] It did not rule on the substance of the litigants' claim that "any packet-mode data provided to a law enforcement agency pursuant to a pen register order will inevitably include some call content, thus violating CALEA's privacy protections."[95] The Court stated that because the TIA had made the initial recommendation and the record showed that the FCC considered the privacy implications, the FCC order was lawful.[96]

This is not to say that the problem has resolved itself. In a recent district court ruling, a law enforcement agency was required to particularly specify to the telecommunications provider what user

---

[89] *Id.* at 456.

[90] *Id.* at 461. The requirement for the FCC to rely on the telecommunications industry for the technical wiretapping standards is found in 47 U.S.C. § 1006(b).

[91] *Id.* at 466.

[92] *Id.* at 453.

[93] *Id.* at 455.

[94] *Id.*

[95] *Id.* at 464.

[96] *Id.* at 465.

information was permissible to be turned over and what was not.[97] The district court acknowledged the difficulties of separating content from signaling information when applied to Internet packet technology. In an interpretation of the pen register statute (47 U.S.C. § 3123), the Court explained their concern: "providers may not be as in tune to the distinction between 'dialing, routing, addressing, or signaling information' and 'content' as to provide to the government only that to which it is entitled and nothing more."[98] Using Internet addresses as an example, the court found that although the IP address a user has visited is permissible to disclose, specific search terms revealed within an Internet address, would constitute impermissibly revealed content.[99]

Privacy advocates also contend that applying CALEA to the Internet may actually encourage the very criminal activities the Order seeks to prevent. Installing access points on the switches and routers that make up the infrastructure of the Internet would make them open for exploitation by third parties.[100] The result ultimately endangers private information kept online.[101]

Landau cites one component of the summary position of the Internet Engineering Task Force ("IETF"). The IETF is the open, international community of researchers who seek to provide standards to the evolution of the Internet's architecture. The organization has expressed doubt over the security of a "tappable" Internet.[102]

> The IETF believes that adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost

---

[97] *In re application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxxxxx@xxx.com]*, 396 F.Supp.2d 45, 49 (D. Mass 2005).

[98] *Id.* at 48-49.

[99] *Id.* at 49.

[100] *See Groups*, *supra* note 22.

[101] *Id.* ("'Once you enable third-party access to Internet-based communication, you create a vulnerability that didn't previously exist,' Marc Rotenberg, executive director at the Electronic Privacy Information Center said in an interview Wednesday. 'It will put at risk the stability and security of the Internet.'").

[102] Landau, *supra* note 74.

> inevitably jeopardizes the security of communications even when it is not being tapped by any legal means.[103]

Landau and the IETF do not doubt it is possible to successfully design a more secure Internet amenable to law enforcement purposes. They, however, do not agree with the propriety of using the architecture of the Internet, as it is today, to create access points because of the inherent security problems it would create.[104] Others, such as Silicon Valley journalist David Cringely, have a dimmer view. Cringely argues that CALEA installations are poorly maintained, lacking adequate security measures such as a firewall, and are open to hacking.[105] For higher education institutions and high-tech companies, the potential unauthorized access of their organization's research presents a relevant concern: "providing another potential conduit for hackers in their products, or stunting privacy and freedom of research could lead to some embarrassing and disruptive episodes."[106]

Privacy, however, is judged under a different standard when it is applied to the Internet, according to supporters of the Order.[107] In a letter supporting the FCC's decision, former Defense Advanced Research Projects Agency Chief, Steve Lucasik, and Anthony Michael Rutkowski, a vice president at Verisign,[108] argue that there is a

---

[103] Network Working Group, *IETF Policy on Wiretapping*, (May 2000) *available at* http://www.ietf.org/rfc/rfc2804.txt.

[104] Landau, *supra* note 74, at 5.

[105] David Cringely, *Shooting Ourselves in the Foot: Grandiose Schemes for Electronic Eavesdropping May Hurt More Than They Help*, I, CRINGELY, http://www.pbs.org/cringely/pulpit/pulpit20030710.html (last visited Jan. 6, 2006) ("The typical CALEA installation on a Siemens ESWD or a Lucent 5E or a Nortel DMS 500 runs on a Sun workstation sitting in the machine room down at the phone company. The workstation is password protected, but it typically doesn't run Secure Solaris. It often does not lie behind a firewall. Heck, it usually doesn't even lie behind a door. It has a direct connection to the Internet because, believe it or not, that is how the wiretap data is collected and transmitted. And by just about any measure, that workstation doesn't meet federal standards for evidence integrity. And it can be hacked. And it has been.").

[106] Jim Duffy, *Higher Ed Fears Wiretapping Law*, NETWORKWORLD (May 1, 2006), *available at* http://www.networkworld.com/news/2006/050106-calea.html?page=6.

[107] The Order does not expressly address the privacy concerns per se.

[108] EFF, *supra* note 23 (the EFF also criticizes the potential role for companies like Verisign, a major operator of domain name root services, as well as Internet security expertise for the FCC, to act as a private, third party surveillance entity).

diminished expectation of privacy once an individual conducts his activities on a public network.[109] Users, however, do expect the government to afford them protections, because of the presence of potential harm that may occur through their interactions on the public network.[110]

VI. THE STATUTORY BASIS FOR APPLYING CALEA TO BROADBAND PROVIDERS

A. BROADBAND PROVIDERS AS A "SUBSTANTIAL REPLACEMENT" FOR TELECOMMUNICATIONS CARRIERS UNDER CALEA

Regardless of the privacy concerns, the legality of the Order is largely dependent on the acceptance of the FCC's statutory construction of CALEA. Critics of the Order argue that Internet providers, in general, have typically been designated as information services under CALEA and are therefore not subject to the law's capacity requirements.[111] The FCC, however, argues that the substantial replacement provision ("SRP") of 47 U.S.C. 1001(8)(b)(ii) recognizes that certain entities, not typically defined as telecommunications carriers under CALEA or the original Telecommunications Act of 1934, can still receive coverage under the statute if they are deemed "substantial replacements" of telecommunications carriers.[112]

Explaining its construction of CALEA under 47 U.S.C. §1001(8)(b)(ii), the Order states how an entity can become a

---

[109] Letter from Steve Lucasik, and Anthony Michael (Nov. 1 2005), *available at* http://scrawford.net/courses/Lukasik-Rutkowski_FCCletter.pdf ("When you use public infrastructures you can not be anonymous because each user interacts with other users and with the system operator: thus we have license plates on cars (plus other information-providing stickers), EZ pass ID for added convenience, operator license attesting to technical qualifications, vehicle VIN, bills of sale and titles, records of transgressions, DOT labeling on trucks, identification of hazardous cargo, etc. So too with providers and users of public networks.").

[110] *Id.*

[111] *See* Joint Comments, *supra* note 54, at 30. "[T]he term 'information services' was shorthand for the Internet and the applications running over it (among other services)."

[112] FCC , *supra* note 1, at 34.

"substantial replacement" of telecommunications carrier using a three-part test:

> a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for the purposes of [CALEA].[113]

The FCC reasons that broadband services engage in "switching or transmission" because the transmission component of the SRP is broad enough to include the packet-mode transport of Internet data.[114] They replace a "substantial portion of the local telephone exchange service" because they are acting as new substitutes for the older, dial-up methods of accessing the Internet.[115] Expressing doubts about the potential negative effect CALEA could impose to technological innovation, the FCC declared that the public interest was served "to safeguard homeland security and combat crime."[116]

CDT ultimately denies that the substantial replacement provision acts as an effective measure for allowing broadband service providers to become telecommunications carriers under CALEA.[117] Contending that Internet providers are information services under 47 U.S.C. § 1001(8)(c)(i), the FCC cannot simply use the substantial replacement provision of 47 U.S.C. § 1001(8)(b)(ii) to trump it.[118]

Other criticisms attack the broad construction the FCC gives to the substantial replacement provision. Accompanying this problem of broadness is vagueness – many entities would not know whether or not they are covered by CALEA.[119]

---

[113] Joint Comments, *supra* note 54, at 5.

[114] FCC, *supra* note 1, at 14.

[115] *Id.* at 15.

[116] *Id.* at 18.

[117] Joint Comments, *supra* note 54, at 25.

[118] *Id.*

[119] *See Summary, supra* note 59.

As detailed in a subsequent section of the article, the D.C. Circuit largely adopted the FCC's interpretation of CALEA.[120]

B. THE LEGISLATIVE HISTORY: SUPPORTS OR COUNTERS THE INTERNET'S EXEMPTION FROM CALEA?

A main argument of the critics of the Order is that the FCC is ignoring the legislative intent of Congress. They point to the language of the House report that accompanied CALEA's passage in 1994:

> The only entities required to comply with the functional requirements are telecommunications common carriers, the components of the public switched network where law enforcement agencies have always served most of their surveillance orders . . . . [E]xcluded from coverage are all information services, such as Internet service providers or services such as Prodigy and America-On-Line.[121]

Citing the House bill, the Electronic Frontier Foundation ("EFF") argues: "The legislative history states that 'all information services . . . [are] excluded from coverage,' and that 'the bill does not require reengineering of the Internet . . . [or] impose prospectively functional requirements on the Internet.'"[122] The FCC is arguably going beyond the bounds of their authority by ignoring the intent of Congress to classify Internet service providers as information services, exempting them from CALEA's coverage.

The FCC's Order, however, in reading the legislative history of CALEA, draws a distinction between the storage of information, as opposed to its transmission. The discussion of information services under the House Report exists to explain only the enhancements of the transmission.[123] Citing the House report, the storage of e-mails would fall within the information services exception of CALEA, while the transmissions of messages would not.

---

[120] *See, infra*, Section VI, C.

[121] Joint Comments, *supra* note 54, at 17 (citing H.R. Rep. No. 103-827).

[122] EFF, *supra* note 23.

[123] FCC, *supra* note 1, at 11.

C. *BRAND X, ACE V. FCC* AND THEIR SUPPORT FOR THE FCC'S CLASSIFICATION SCHEME

The Supreme Court's recent holding in *Brand X* provides some insight into the extent of the FCC's authority to classify and regulate cable providers under CALEA.[124] The outcome of the legal battle between the FCC and opponents of the Order provided legal weight in favor of the FCC. The Court ruled that the FCC made a reasonable interpretation that cable companies that were providing broadband Internet services were *not* telecommunications carriers.[125] As a result of this holding, the cable companies are not entities resembling common carriers, and are subjected to less regulation by the FCC. They do not have to share their lines with other Internet service providers.[126]

The holding initially presented some tension between the FCC's classification of broadband providers under the 1996 Telecommunications Act and CALEA. The FCC argued successfully in *Brand X* that broadband providers were information services under the Telecommunications Act. In the current Order, however, the agency proposes that the same providers are telecommunications carriers under CALEA.[127] Observing the specific language of *Brand X*, however, the Order states,

> In reaching its decision, however, the Court recognized that cable modem service does contain a telecommunications transmission component that is integrated with the information service capability.... Thus, cable modem service is subject to CALEA under the SRP.[128]

The majority found that between two possible constructions of a statute, an agency is granted deference to its opinion on which

---

[124] Nat'l Cable and Telecomm. Ass'n. v. Brand X Internet Servs., 125 S. Ct. 2688 (2005).

[125] *Id.* at 2704.

[126] *Id.*

[127] FCC *supra* note 1, at 14 n. 76.

[128] *Id.*

construction is accurate.[129] The implication of this holding bodes favorably for the FCC; the agency's opinion about whether broadband providers are telecommunications carriers or information services would be entitled to greater deference[130]

The D.C. Circuit has already granted the FCC a favorable opinion in *American Council on Education (ACE) v. FCC.*[131] In a 2-1 decision, the majority ruled that the FCC's argument based on the substantial replacement provision of CALEA allowed broadband and VoIP services to fall under its coverage.[132] The D.C. Circuit distinguished the FCC's accepted argument that broadband providers were "information services" under the 1996 Telecommunications Act in *Brand X*, versus the argument that broadband providers were not "information services," excluded from CALEA coverage.[133] It also adopted the Supreme Court's reasoning in *Brand X* which provided deference to the FCC's interpretation of a statute so long as it appears reasonable: "ACE's analysis is inconsistent with our standard of review. We cannot set aside the Commission's reasonable interpretation of the Act in favor of an alternatively plausible (or an even better) one."[134]

---

[129] *Brand X*, 125 S. Ct. at 2704. ("Where a statute's plain terms admit of two or more reasonable ordinary usages, the Commission's choice of one of them is entitled to deference"). The Court held that the FCC's construction was permissible after applying the two-step test of Chevron, U.S.A., Inc. v. NRDC, 467 U.S. 837 (1984).

[130] *Brand X* was not without its detractors. Justice Scalia's dissent criticized the FCC's "implausible" construction of the Telecommunications Act of 1996, which suggests that future litigation for the FCC may not automatically provide another favorable result ("The Federal Communications Commission (FCC or Commission) has once again attempted to concoct 'a whole new regime of regulation (or of free-market competition)' under the guise of statutory construction.... The important fact, however, is that the Commission has chosen to achieve this through an implausible reading of the statute, and has thus exceeded the authority given it by Congress"). *Id.* at 2713.

[131] Am. Council on Educ. v. FCC, 451 F.3d 226, 235 (D.C. Cir. 2006).

[132] *Id.*

[133] *Id.* at 232. The D.C. Circuit noted the differences between the two acts: "ACE's syllogism falls apart because CALEA and the Telecom Act are different statutes, and *Brand X* was a different case. Although ACE would have us read *Brand X* was controlling this controversy, that case did *not* hold that broadband Internet access is exclusively an 'information service,' devoid of any 'telecommunications' component. Rather, it upheld the *FCC's* reasonable interpretation to that effect under a *different statute.*"

[134] *Id.* at 234.

Notably, the D.C. Circuit explicitly ruled that CALEA does not apply to private networks.[135] ACE has used this language to argue that higher education institutions, which it argues largely rely on private Internet connections, are not affected by the Order.[136] CALEA specifically exempts "equipment, facilities, or services that support the transport or switching of communications for private networks or for the sole purpose of interconnecting telecommunications carriers."[137] ACE believes that because most colleges and universities do not predominantly offer its Internet connections to the public, it is exempt from CALEA compliance.[138] The D.C. Circuit, however, did not consider to what extent the FCC's proposed order covers private networks interconnected with networks covered under CALEA, finding that the issue was not ripe.[139] Clarification of this issue is expected – the D.C. Circuit granted ACE's petition to rehear its argument.[140]

VII. CONCLUSION

The FCC has formulated a unique statutory argument to rationalize their application of CALEA to the Internet. Statutory construction has thus far determined the outcome of the suit filed against the Commission. Considerations of privacy, although implicated in important ways by CALEA, will not likely represent an outcome-determinative element in any subsequent court proceedings. In light of the statutory deference afforded to the agency under *Brand X*, the FCC's statutory interpretation may rest on more solid ground. The

---

[135] *Id.* at 236 ("The *Order* on review--like CALEA--expressly excludes "private networks" from its reach.").

[136] *Application, supra* note 12.

[137] 47 U.S.C. § 1002(b)(2)(B).

[138] *Application, supra* note 12 ("Thus, campus networks that offer Internet connectivity but are made available only to students, faculty, and administrators—and that exclude the public at large, for example by requiring university ID cards to gain access to networked terminals and by requiring password authentication on wireless networks, among other measures—almost certainly would be considered private.").

[139] Am. Council on Educ, 451 F.3d at 235-236.

[140] *Court to Revisit VoIP Wiretap Ruling*, TELECOMWEB (Aug. 7, 2006), *available at* http://www.telecomweb.com/tnd/18532.html.

outcry by certain organizations, such as higher education institutions concerning the cost of implementing CALEA, may force the issue back to the legislature. Although the FCC's next decision on CALEA, which would concern the implementation of the plan, may exempt certain organizations from full compliance with the Order, it does not appear that the FCC will back down from their decision as a whole. The privacy issue will become a battle over public policy.